EUROPOL

Freedom AND Security

Killing the zero sum process #kill0sum

EDEN Conference Report

Freedom AND Security / 22-23 November 2018

EDEN

ERA

EUROPOL PUBLIC INFORMATION

Table of contents

Welcome address of the Executive Director of Europol

Catherine De Bolle
Executive Director

For quite a long time already now, there has been an intense public debate about the right balance between individual freedom, such as the right to data protection, and public security. The protection of personal data and public security are at the core of the present discussion. They are often considered to be conflicting aspects of this debate. But what is the exact public interest in this context?

We at Europol recognise the necessity to talk about dignity and respect for fundamental rights when fighting transnational crime and terrorism. But, how can law enforcement effectively respond to terrorist and cybercrime threats when at the same time protecting the fundamental right of data protection? How much of our privacy will we, or should we, sacrifice in order to guarantee security? Do we actually need to sacrifice privacy and freedom in order to guarantee security?

These are only a few of the questions that come to mind when addressing the debate about the right to privacy, and the right to security, in the digital age. I would like to discuss this issue without opposing the two concepts. It is important to show that the legal and security justifications in the recurrent controversy can both be upheld.

We do not have to choose either freedom or security. There is no need to compromise on individual privacy for the sake of public security.

In the fulfilment of our mandate we at Europol are working to increase the synergies between these two fundamental rights. Indeed, this conference is not just about the link between the work of law enforcement and the impact it might have on fundamental rights. It is ultimately about transparency.

The message I would like to give to you today is: here at Europol we work hard to do our job in the right way. We are determined to make Europe a safer place, and full compliance with fundamental rights in Europol's activities is a part of this safer Europe. When it comes to Europol's mission the right to data protection is probably the most important one. And this fundamental right is in the public focus, especially in Europe with its data protection reform.

Earlier this year the GDPR – the General Data Protection Regulation – entered into force. With it, came a reform package which included the Data Protection Directive for the Police and Criminal Justice Sector – the so-called Police Directive. Our discussion today must and will start from there!

We firmly believe that the harmonisation of the data protection rules is a positive development which in many ways facilitates cross-border cooperation between police and justice authorities, both within the EU and with international partners. However,

the practical implementation of these innovative legal frameworks takes time, effort and sometimes also causes complications. The developments around the access of law enforcement to WHOIS information that you will hear about at the beginning of this conference are just one example.

Another interesting question is how a proportionate and harmonised data retention regime at EU level could be designed building on the criteria defined by the European Court of Justice. Furthermore, a conversation about data protection in the law enforcement sector could never be exhaustive without considerations on current cyber-threats. Ransomware, as well as the trading of illegal commodities on the Darknet, represent fundamental challenges for law enforcement. Only if law enforcement, the private sector and the academic world work together closely, will cybercrime be tackled effectively.

Let us listen to each other and let us work to overcome the zero-sum process.

Let us increase both Freedom AND Security!

Introduction

Not a conventional data protection conference…

Being at Europol Headquarters is an inspiring experience per se. From the outside, the building resembles a fortress of reinforced concrete. CCTV cameras at every corner as well as guards eagerly patrolling the building put an emphasis on security

However, once the participants of the conference "Freedom AND Security – Killing the zero-sum process" entered the auditorium, they were welcomed with colourful armchairs on stage, while footage of highly skilled surfers on monumental waves was projected on the wall. At the end of the clip the word "Freedom" appeared, almost challenging the silvery Europol logo in the background.

"Many of you coming into this room wondered surely what is this actually about? Is this a surfers' conference?" said Daniel Drewer - Data Protection Officer of Europol welcoming participants including law enforcement officers, academics, representatives of NGOs, private enterprises and many more. "Those of you who are not from The Hague, and those of you that are here for the first time should know that this Auditorium is less than two kilometres away from the sea."

"What we did before the conference, when we looked at the title 'Freedom AND Security', was asking the surfers at Scheveningen Beach what 'Freedom' is for them. Because everybody has a different perception of freedom, and a surfer's view on freedom is among the most inspiring. What they did was provide us with this clip."

The idea behind this conference was that any notion of balancing "freedom versus security" wrongfully implies a unitary dial: if we turn up freedom, we get less security, and if we turn down freedom, we get more security. Freedom and security are viewed as a zero-sum trade-off. There is no doubt that there is a relation between freedom

and security: A change to one will sometimes affect the other. But often it is also possible to increase security without decreasing freedom, and sometimes a decrease in our freedoms leads to no meaningful increase in security.

The EDEN conference aimed at developing a platform for an open discussion on the topic of data protection in a law enforcement context. In order to do so, many assumptions and prejudices needed to be challenged. This report will go through some of the highlights of the conference demonstrating its uniqueness and originality.

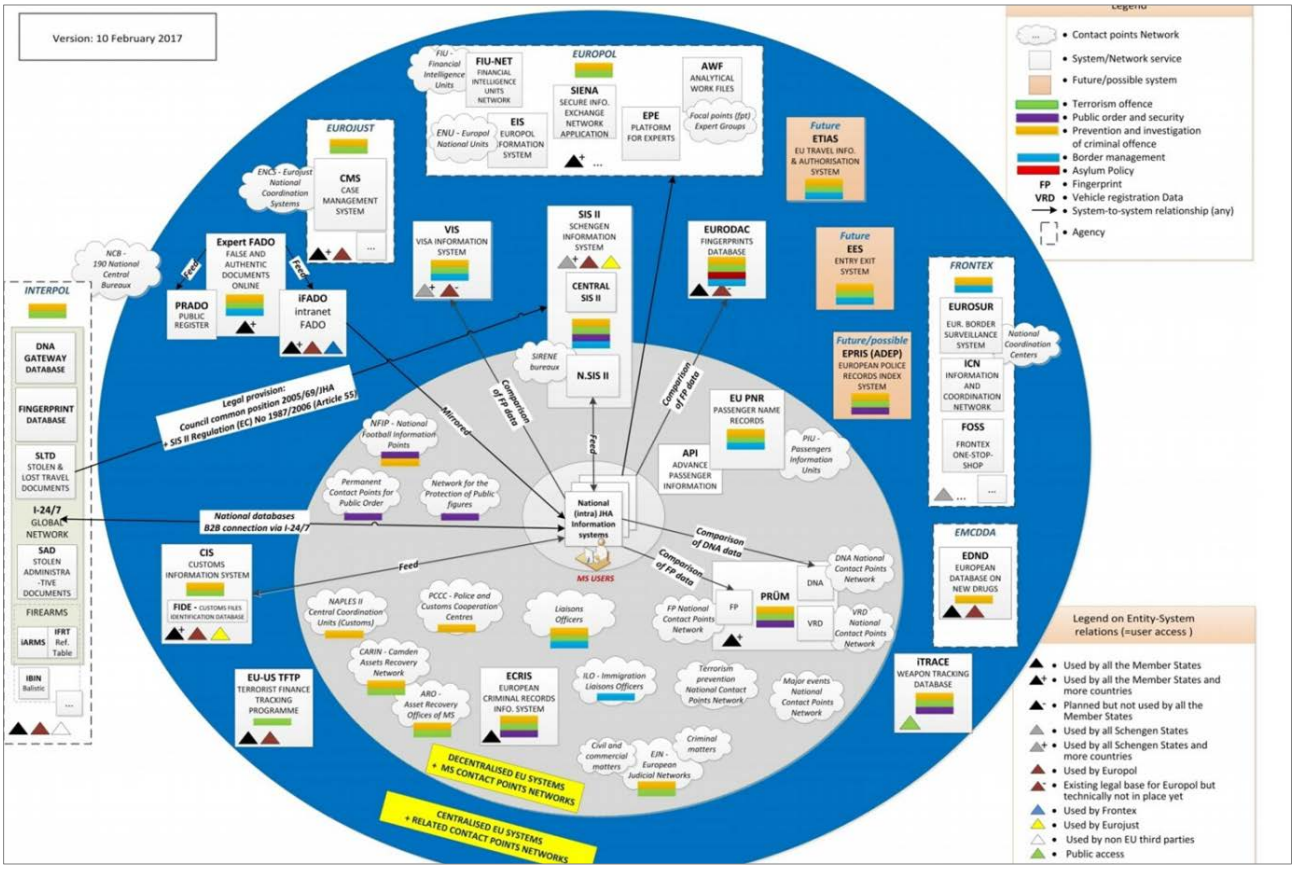
Daniel Drewer
Data Protection Officer

Keynote of the Assistant Supervisor at the EDPS

The current information exchange and information management environment in the Justice and Home Affairs area shows an increase in interoperability of databases in the law enforcement sector. Not all of them are interconnected at present, but there is the necessity to be ready for the moment in which all of them will be interoperable. With more and more personal data being processed through the same information systems and networks, cyber-security must not become an excuse for disproportionate processing of personal data.

The need for special rules in data protection for Europol, as outlined by its regulation, has always been recognised as highly valuable. It represents a practical approach that allows privacy and cybersecurity to be put on the same side. There is no privacy protection without security, and security does not exist without privacy protection and data protection. They are both in the same amalgam that aims to create the strong basis for the protection of fundamental rights in the European Union.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. A number of specific duties of the EDPS are laid down in Regulation 45/2001 (now Regulation 2018/1725).



Overview of the information exchange environment in the justice and home affairs area, Council SecGen - 15.2.2017, 6253/17, p.3 https://db.eurocrim.org/db/en/doc/2698.pdf

Privacy and data protection are fundamental rights

Independent supervision is an integral part of the right to data protection – Article 16(2) TFEU and 8(3) Charter of Fundamental Rights.

The tasks of the EDPS include:

- Monitoring and verifying compliance with Regulation (EC) 45/2001, (**Supervisory Tasks**);
- Promoting data protection awareness, design, and development;
- Giving advice to controllers, (**Consultative Tasks**);
- Advising the co-legislators on new legislation;
- Cooperating with Member States' DPAs, (**Cooperative Tasks**);
- Handling complaints, conducting inspections;
- Monitoring technological developments;

"We are standing on the same side, we are both from the same sector dealing with freedom and security in the European Union. This is not the ideal, philosophical solution: this is the practice of the work of the data protection authorities. I guess one third or maybe half of the people who are working in data protection authorities have been working before in the security sector. I have also myself the experience of working in the Ministry of Interior of my country of origin."

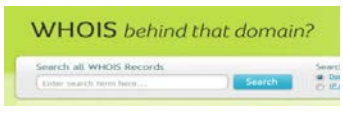
Wojciech Wiewiórowski
Assistant Supervisor at the EDPS

Panel 1:

Impact of GDPR on law enforcement: the WHOIS story

The Internet Corporation for Assigned Names and Number (ICANN) is 'a not-for-profit, public-benefit organisation' that coordinates domain names at a global level, assigning unique identifiers, such as IP addresses, and accrediting generic top-level domain (gTLD). Until the application of the GDPR in May 2018 the WHOIS is a publicly available and decentralised database of registration and contact information of the retailers and owners of domain names; it is 'the system that asks the question, who is responsible for a domain name or IP address?' The WHOIS data can include 'name, address, email, phone number, and administrative and technical contacts'.

For many years, law enforcement agencies (LEAs) have relied on the WHOIS to investigate and attribute crime online such as: spam, phishing, malware, C2, BPH, ransomware, counterfeit products, child sexual abuse material, and terrorist propaganda. It allowed LEAs to make correlations and patterns that led to the owners of a domain. This tool represented one of the few active elements of online accountability and was also used by judicial authorities, customs, CSIRTs, IP right holders, cybersecurity researchers, etc.



An example of the use of WHOIS was 'AMAQ', a case about terrorist propaganda being spread via social media and websites. The case lasted more than two years, and it allowed the identification of 413 domains. Without the information obtained through WHOIS, the investigation would have been blocked since the very beginning and no takedowns would have taken place.

Since 2003, data protection authorities (especially the Working Party Article 29) have taken issue with the public availability of the personal data contained in WHOIS, offering guidance to ICANN on how to bring WHOIS in compliance with European data protection law. On the 25th of May 2018, ICANN introduced a 'Temporary Specification' that aimed at making the WHOIS policy GDPR-compliant. 'Reasonable access' must now be requested in order to disclose non-public information.

The panel tried to demonstrate that the compliance issue of the WHOIS database with data protection rules has been discussed well-before the applicability of the GDPR. The law enforcement perspective has shown that the current situation will represent a significant obstacle regarding the identification of unknown and newly-established online criminal infrastructures. The legitimacy and importance of access to WHOIS data for law enforcement purposes is uncontested by the Commission which has communicated to ICANN the dual objectives of ensuring quick access to its directories for public interest purposes whilst being fully compliant with EU data protection rules.

"The WHOIS story shows a tension between traditional decision-making processes based on sovereignty and the global multi-stakeholder governance model that regulates the internet. The real challenge is to implement data protection rules in the multi-stakeholder environment."

Gregory Mounier – Head of Outreach and Prevention Team, EC3, Europol

"It is our task to find those bad guys back in the days when they were noobs, when they were young guys testing. It is our task to find the mistakes they made in the past and to attribute those to their wrongdoings at this very day."

Mirko Manske – Teamlead of Cyber Intelligence Operations, BKA

"GDPR is not the problem. The problem is now that law enforcement agencies live in an era of legal uncertainty when they need privately-owned data. There should be a common agenda, a shared urgency, to come up with a unified access model as soon as possible."

Cecilia Verkleij – Deputy Head of Unit Police Cooperation and Information Exchange,

Panel 2:

Data as the new oil? Risks and opportunities for citizens and law enforcement

Images and metaphors often allow us to better express concepts in a more "user-friendly" way. The claim "Data is the new oil" is one of these metaphors. It suggests that data is a valuable commodity with many different uses across many applications. It is commonly credited to Clive Humby, a British mathematician in charge of setting up a commercial loyalty programme who highlighted the fact that, although inherently valuable, data needs processing, just as oil needs refining before its true value can be unlocked.

According to some, data is the new oil because it drives companies worldwide, generating a new lucrative and fast-growing industry. This argument is put forward to show, for example, that as much as oil in the last century induced antitrust regulators to restrain the controllers of its flow, the same should be done with data. Indeed, as much as in the era of oil the control of resources gave enormous powers to energy companies, today in a data-driven economy the power of Internet companies is increasingly important.

The analogy with oil has, however, also been criticised and rejected due to important differences. Oil requires huge amounts of resources (including oil itself) to be transported to where it is needed, data, on the other hand, can be moved around the world at the speed of light, at very low cost, through optical fibre networks. While oil is a finite resource, data is effectively infinitely durable and reusable. While oil cannot regenerate itself, data does indeed generate both new data and metadata.

This panel highlighted that, although metaphors like "Data is the new oil" can be useful in making technologies less obscure to the general public, it is more important to raise awareness of the rights and responsibilities of the citizens, enterprises, and governments handling personal data in today's world.

"The main striking difference between data and oil on my point of view is that the misuse of data carries a complex variety of unknown dangerous complications."

Jyn Schultze Melling – Associated Partner, Ernst & Young

"While security means being free from intentionally caused harm, safety means being free from unintentional accidents. For a conversation on the relationship between privacy and security to be complete, it needs to include considerations on safety."

Els De Busser – Assistant Professor Cyber Security Governance, Leiden University

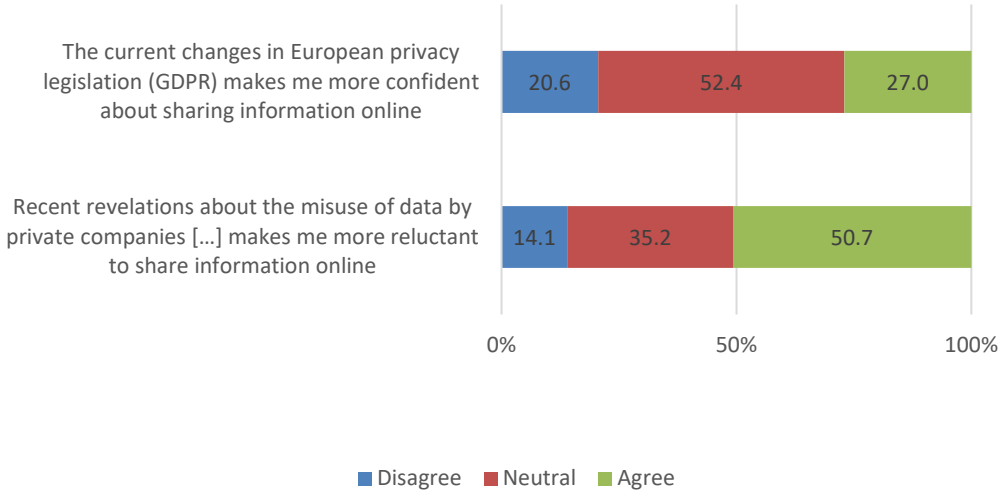
"Data is not an asset, it is a liability. Data is not the new oil, it is the new asbestos!"

Ralph Bendrath – Senior Policy adviser to MEP, European Parliament

"We are not communicating properly to citizens what is the use that we do with their data. Hence the issue of mistrust is constantly popping up."

Babak Akhgar – Professor of Informatics, Head of CENTRIC, Sheffield Hallam University

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

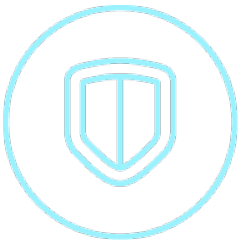


Panel 3:

Data as the hostage – ransomware is still alive!

According to the Internet Organised Crime Threat Assessment (IOCTA) 2018, ransomware dominated reporting across the boards throughout 2017, from media to law enforcement and from the financial sector to the security industry. Even though the growth of ransomware is beginning to slow down, it still remains one of the most prominent malware threats overtaking banking Trojans in financially-motivated malware attacks. The WannaCry and NotPetya attacks of mid-2017 were of an unprecedented global scale, affecting an estimated 300.000 victims worldwide. Within the European Union, the attacks have targeted a wide range of critical infrastructures and key industries, affecting health services, telecommunications, transport and manufacturing industries.

While there continues to be a global coordinated response to these specific attacks, European law enforcement reports ransomware attacks from a wide range of other ransomware families. The most commonly reported are Cerber, Cryptolocker, Crysis, Curve-Tor-Bitcoin Locker, Dharma and Locky. Overall damages arising from ransomware attacks are difficult to calculate, although some estimates suggest a global loss in excess of USD 5 billion in 2017. Furthermore, it is important to highlight the huge disparity between the losses of singular victims compared to the actual criminal revenue generated.



The illegal acquisition of data following data breaches is also a prominent threat. Criminals often use the obtained data to facilitate further criminal activity. In 2017, the biggest data breach concerned Equifax, affecting more than 100 million credit users worldwide. Data is the lifeblood for almost any industry and this makes it the favoured target of attacks aimed at illegally acquiring, destroying or denying access. Industry reports that personal data is most commonly compromised, followed by payment data and then medical data.

This panel highlighted the persistent threat by ransomware. New legislation relating to data breaches will likely lead to greater reporting to law enforcement. The GDPR makes

the notification of data breaches a legal requirement across the EU subject to significant fines. Some argue that this may give rise to scenarios where hacked companies would rather pay the smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by the competent authority.

"A harmonised and proactive approach to vulnerabilities could really help deterring ransomware proliferation, maybe contributing also to law enforcement response to these threats. Furthermore, by discussing vulnerabilities we will be able to redefine two important concepts: government accountability and trust in the cyberspace."

Stefano Fantin – Legal and Policy Researcher, Centre for IT & IP Law, Catholic University of Leuven

"What will be crucial for law enforcement authorities is how data protection authorities will enforce and supervise the rules of the Directive. While for the GDPR we have a very clear framework on supervision and enforcement, including the threat of administrative fines, for the Directive it is quite vague how supervisory authority will make law enforcement authorities respect those rules."

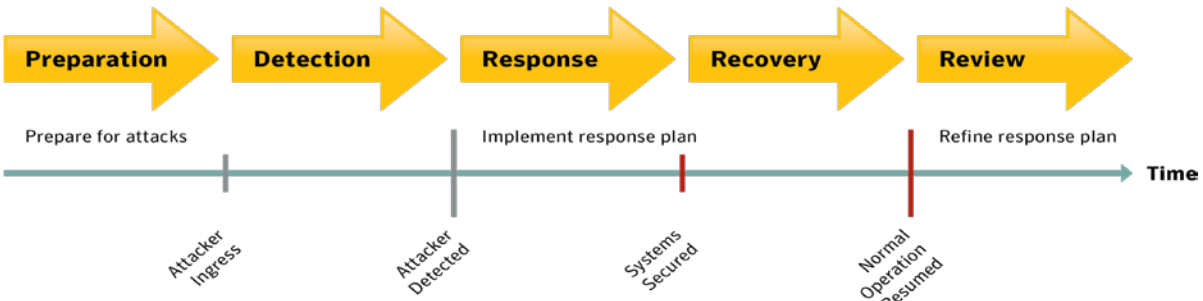
Juraj Sajfert – Policy Officer, Data Protection Unit, DG Justice and Consumers, European Commission

"Ransomware is changing nature. It is starting looking also into senior executives, because senior executives are the people that should play a role in the current ecosystem when we want to create a more cyber-resilient environment."

Francesca Bosco – Project Lead, Cyber Resilience Team, World Economic Forum's Center for Cybersecurity

"Managing the rights and privileges of users within an organisation is the key to stop the impact and spread of malware. Two of the key principles of security are very often overlooked and they are really critical to stop the spread of ransomware within an organization: the principle of need to know and the principle of less privilege."

Rik Ferguson – Vice President Security Research, Trend Micro



Source: "The Cyber Resilience Blueprint: A New Perspective on Security"

Panel 4:

The take-down of Hansa – at times the Darknet ain't that dark!

Darknet markets are a key crosscutting enabler for other crime areas, providing access to – amongst other things – compromised financial data to commit various types of payment fraud, and fraudulent documents to facilitate fraud, trafficking in human beings, and illegal immigration. While an unprecedented number of users are now making use of Tor, the Darknet is not yet the mainstream platform for the distribution of illicit goods. However, it is rapidly growing its own specific customer base in the areas of illicit drugs, weapons, and child sexual exploitation material. Compared to more established Darknet market commodities, such as drugs, the availability of cybercrime tools and services on the Darknet appears to be growing relatively fast.

In 2017, two major law enforcement operations - led by the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol - have shut down the infrastructure of an underground criminal economy responsible for the trading of over 350,000 illicit commodities including drugs, firearms and cybercrime malware. This coordinated law enforcement action in Europe and the US ranks as one of the most sophisticated takedown operations ever seen in the fight against criminal activities online.

Europol has been supporting the investigation of criminal marketplaces on the Dark Web for a number of years. With the help of Bitdefender, an internet security company advising Europol's European Cybercrime Centre (EC3), Europol provided Dutch authorities with an investigation lead into Hansa in 2016. Subsequent enquiries located the Hansa market infrastructure in the Netherlands, with follow-up investigations by the Dutch police that led to the arrest of its two administrators in Germany and the seizure of servers in the Netherlands, Germany and Lithuania. Europol and partner agencies in those countries supported the Dutch National Police to take over the Hansa marketplace on 20 June 2017 under Dutch judicial authorisation, facilitating the covert monitoring of criminal activities on the platform until it was shut down. In the meantime, an FBI and DEA-led operation, called Bayonet, was able to identify the creator and administrator of AlphaBay, a Canadian citizen living a luxurious life in Thailand. On 5 July 2017, the main

suspect was arrested in Thailand and the site taken down. Millions of dollars' worth of cryptocurrencies were frozen and seized.

Going through the specificities of these operations, this panel demonstrated that the take-down of Hansa and Alphabay represented a ground-breaking example for investigations in the Darknet. Not only its effectiveness made it a success story, but its impact was even more meaningful because it contributed substantially to the demystification of the Darknet.

"According to a Dutch research organization, TNO, this was 'a game changing police intervention' because it was the first time an operation impacted on the trust of users on the Darknet."

Nils Andersen Röed – Project Leader, Dark Web Unit, Dutch National Police

"An effective approach to cyber criminality is a combination of: knowing what the criminal business model looks like; identifying the value-chain that drives that business model; and designing evidence based interventions, aimed at disrupting the criminal business model, taking on the facilitators, arresting the perpetrators, mitigating the impact of the criminality and minimising the opportunities to monetise on the attacks."

Lodewijk van Zwieten – Cybercrime Prosecutor, Dutch Public Prosecution Service

"Operation Bayonet has been the turning point also in terms of how it was presented in the media and perceived by the public. Since then the chatter on the Darkweb is that no one can trust each other anymore."

Victoria Baines – Visiting Associate, Oxford Internet Institute, University of Oxford

Panel 5:

The death of data retention at EU level – the mass surveillance scandal fallout and its detrimental consequences for law enforcement

Following the annulment of the Directive 2006/24/EC on Data Retention (DRD) by the Court of Justice of the EU (CJEU) in April 2014 due to a lack of proportionality (Digital Rights Ireland), and the Tele2 ruling in December 2016 according to which also Article 15 of the ePrivacy Directive 2002/58/EC cannot serve as a legal basis for data retention, law enforcement and judicial authorities face enormous challenges in investigating online crime.

According to the standards set out by the CJEU, data retention-collection-storage:

- May not happen on a generalised basis;
- May not be indiscriminate;
- May not be bulk-collection;
- Must be limited to what is strictly necessary;
- Requires differentiation, limitation or exception in light of the objective pursued;
- Must be targeted (at least not fully untargeted; scope for 'relatively untargeted');
- Must be limited to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons;
- Must be limited with respect to (cumulatively):
- The categories of data to be retained,
- The means of communication affected,
- The retention period adopted,
- The 'persons concerned' or 'the public that may potentially be affected';
- Must be defined on the basis of the objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one,

with serious criminal offences, and to contribute in a way or another to fighting serious crime or to prevent a serious risk to public security;
- Does not need to amount to 'reasonable suspicion'.

This panel displayed a passionate debate amongst those who deem data retention an indication for the rise of a police state versus those who consider it indispensable in the fight against serious crime and terrorism. A key message conveyed was that law enforcement is not advocating the general or indiscriminate retention of any available information, but is making best efforts to implement the criteria established by the ECJ. Nonetheless, it aimed at raising awareness on the severe detrimental consequences of the status-quo.

"It is clear that the Court has left an opening for fundamental rights, compliance and a data protection regime to be established, and it is also very clear that European law enforcement agencies would like to see such legislation adopted. The question is whether the current EU institutional makeup is capable of delivering such regime."

Ben Hayes – Fellow, Transnational Institute

"I think that everybody recognises the need for tools for law enforcement to combat serious crimes, but on the other hand the necessity to safeguard people's fundamental rights."

Henrik Saugmandsgaard Øe – Advocate General of the Court of Justice of the EU

"If in real life crimes law enforcement agencies have the power to recognise people near the crime scene, why in the electronic world this should be any different?"

Ilmari Viro – Head of Special Operations, Telecommunication Unit, Finnish National Bureau of Investigations

"With a bit of creativity, it is possible to come to a good set of selectors which make your life easy for the future. Not as easy as receiving everything without having to do anything, but my invitation is: why don't you give it a try?"

Gert Vermeulen – Professor of Criminal Law, Ghent University

Panel 6:

If you can make it there, you can make it anywhere – data protection by design for cooperation between law enforcement and intelligence services?

The attacks that have shocked Europe in recent years have demonstrated an evolution in both the modalities and the schemes of the terrorist threat. On the one hand, considering their planning, their means and modalities, these attacks have increasingly acquired similar traits with well organised warlike activities. On the other hand, phenomena driven by the actions of a single terrorist, "lone wolves" or "foreign fighters", have challenged the way terrorism can be prevented and fought due to the increased integration of the attackers in the attacked environment. The metamorphosis and versatility of the phenomenon has brought to the necessity of an increased cooperation between all the interested stakeholders in the fight against terror.

Both law enforcement agencies and intelligence services across the world hold valuable information which can facilitate the fight against terrorism. However, the willingness to enter more intense cooperation is still limited also due to historical rivalries and reluctances. For example, in the law enforcement community many intelligence services have a reputation of wanting to receive all available information, but not being willing to share anything in return. Even if "the need to share" became common practice, there would still be a lot of issues to be sorted out, many of which have a data protection component.

This panel tried to build bridges between all stakeholders in order to enable the right choices on issues such as encryption and confidentiality of communication, purpose limitation and effectiveness of measures, rule of law by design, bulk surveillance, and deployment of the appropriate resources for independent and effective oversight of the activities of Intelligence Services and Law Enforcement Agencies.

"Law enforcement is carrying out and fulfilling the protection duty of the State for human rights. Law enforcement is from the very beginning not the enemy or the threat for human rights, but basically it is the one field where human rights should be protected in practice, not just normatively."

Christof Tschohl – Scientific Director, Research Institute, Digital Human Rights Centre

"We at FRA believe that increasing intelligence oversight, both at national and at international level, is clearly a vital challenge for the years to come. But I think it is really the only way where we can ensure that the exchange of data between law enforcement and intelligence services can be conducted in a proper way in line with the rule of law."

Mario Oetheimer – Head of Sector, Information Society, Privacy and Data Protection, Fundamental Rights Agency

"Trust is a very important part of the work we do. Not just between the services but also between our services and international partners we work with. With everything that is going on in the world at the moment and the global threats we are facing, it is impossible to do the work we do on our own."

Erwin Smit - Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

"You are seeing history being made today. The fact that we have the Dutch Intelligence Agency with us here is history being made. […] We are discussing things that until quite recently it was almost forbidden to discuss."

Joe Cannataci – UN Special Rapporteur to the Right to Privacy

Panel 7:

From law enforcement fiction to future – will there be any privacy left in 2030, anyway?

Science fiction is a genre of speculative fiction typically dealing with imaginative concepts. Its readers are trained to anticipate the unexpected and helped to face change in a future that will radically differ from the present. Rick Deckard, RoboCop, and Judge Dredd are only a few examples of science fiction's recurring inspiration from the world of law enforcement.

According to Arthur C. Clarke: "Science fiction seldom attempts to predict the future. More often than not, it tries to prevent the future."

Concerning data protection, there are two paths ahead of us. One is a dystopian future worthy of the most frightening episode of Black Mirror. The other involves a cultural revolution that will require collective efforts and shared responsibilities in order to protect individual's freedoms and fundamental rights.

On the one hand, there is personalized pricing, credit scoring, forced consent, micro-targeted ads leading to micro-targeted news and to micro-targeted political campaigns. Probably even more frightening, there is the use of opaque technological advancements for global mass surveillance purposes.

On the other hand, there is collectivised privacy enforcement, the European-Californian effect spreading data protection regulations worldwide, and a cultural shift that will no longer leave responsibilities only on the users. The implementation of privacy by design together with the respect of data protection considerations by law enforcement will allow us to kill the zero-sum process between privacy and security.

By showing the possible alternative futures, this panel aimed at debating not only what should be Europe's next moves in enhancing data protection, but looked beyond European borders to understand current trends and strategies.

"The question of enforcement is often the crucial question when talking about the future of privacy. We should make sure that we enforce our rights, not just have them on paper."

Max Schrems – Privacy Advocate , Chairman, None of Your Business (NOYB)

"EU is not having this kind of moral high ground with privacy anymore, as it used to be. Companies are not anymore in the position to follow the legislation, they are in the position to make decision on which regulation they prefer violating."

Mika Lauhde – Vice President Cyber Security & Privacy, Huawei Technologies

"DPO activities are not just about the protection of personal data, they are enabler of data driven law enforcement activities in the future. They will increasingly help enhancing the trust in institutions."

Hiroshi Miyashita – Associate Professor, Chuo University

"We are all active players. The question of the panel should be reformulated in an active way: What can each of us do for privacy to be alive and kicking in 2013?"

François Pellegrini – Commissioner, National Commission for Information Technology and Civil Liberties (CNIL)